ETH-XMR Atomic Swaps

Monerotopia April 2022

about me

- Elizabeth
- blockchain protocol developer for 4+ years

summary

- motivation
- ETH-XMR atomic swap development progress
- protocol deep dive (maybe)
- demo (~8mins)
- privacy and security implications
- next steps for research and development

demo

atomic swaps vs bridges vs exchanges

- Exchanges
  - Centralized, trusted, custodial
  - All info (addresses, KYC) revealed to the exchange
  - No privacy from the exchange and regulators, but potentially more privacy from your neighbour
- Bridges
  - Range from centralized to decentralized
  - Addresses, amounts generally revealed on-chain
- Atomic swaps
  - Fully decentralized, peer-to-peer, trustless
  - Addresses, amounts generally revealed on-chain (unless?)

motivation

- Ethereum is the largest blockchain by usage
- increases Monero accessibility
- potential for DeFi integration

the project

- created a protocol for atomic swaps between ETH-XMR
- uses a smart contract to manage claims/refunds
- current implementation being developed in Go
- Notable codebase features:
  - Go ed25519 library for Monero
  - networking in libp2p; includes DHT for peer discovery

development progress

M1: Feature completion + test coverage - DONE

M2: Swap contract “factory” for gas savings - DONE

M3: DLEq integration for gas savings - (mostly) DONE

M4: Integration (E2E) testing - DONE

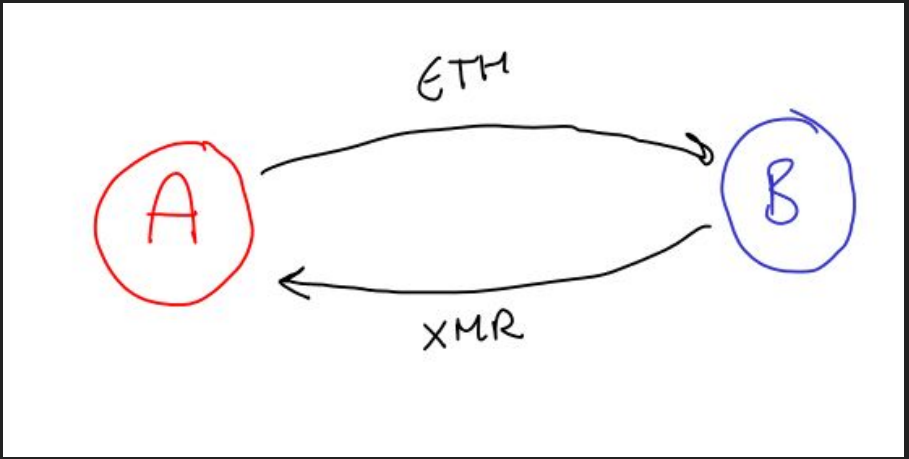
M5: Stagenet testing + infrastructure setup - in progress

M6: SwapV2 research + write-up - in progress

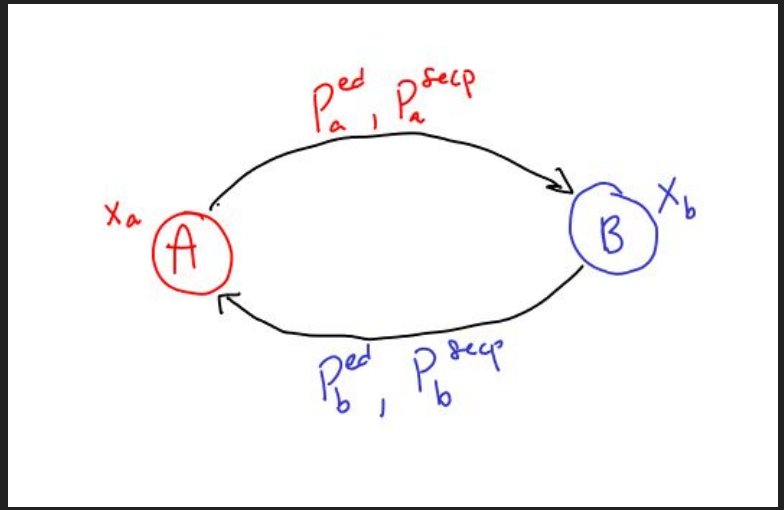
M7: UI - in progress

the protocol: happy path

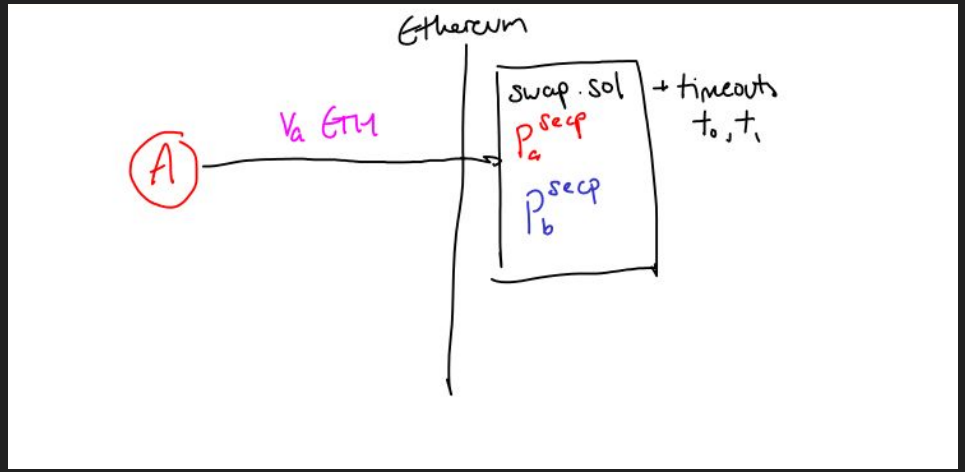
- Alice: has ETH, wants XMR
- Bob: has XMR, wants ETH



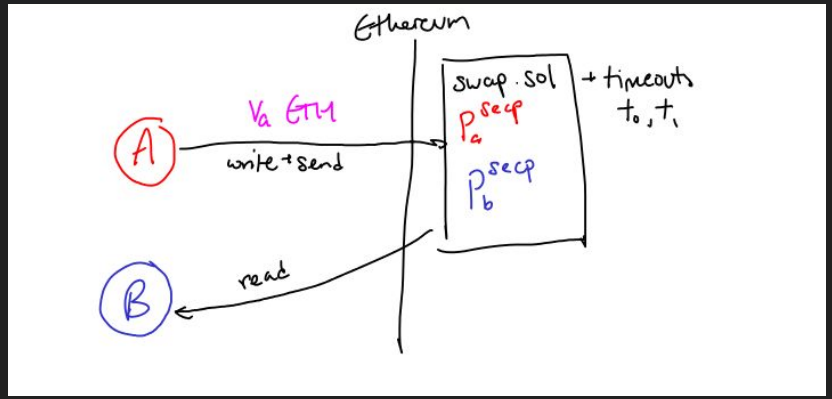
1. Alice and Bob meet and agree on the amount to swap
    a. They generate one-time swap secret keys `x_a` and `x_b`
    b. From their secret, they each generate a secp256k1 key (for Ethereum) and an ed25519 key (for Monero)
    c. They send these to each other over the network

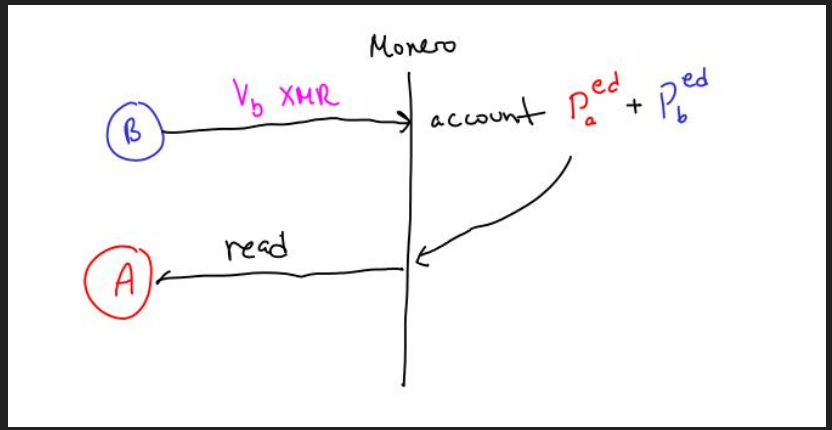


2. Alice locks ETH in a smart contract that stores secp256k1 `P_a` and `P_b`



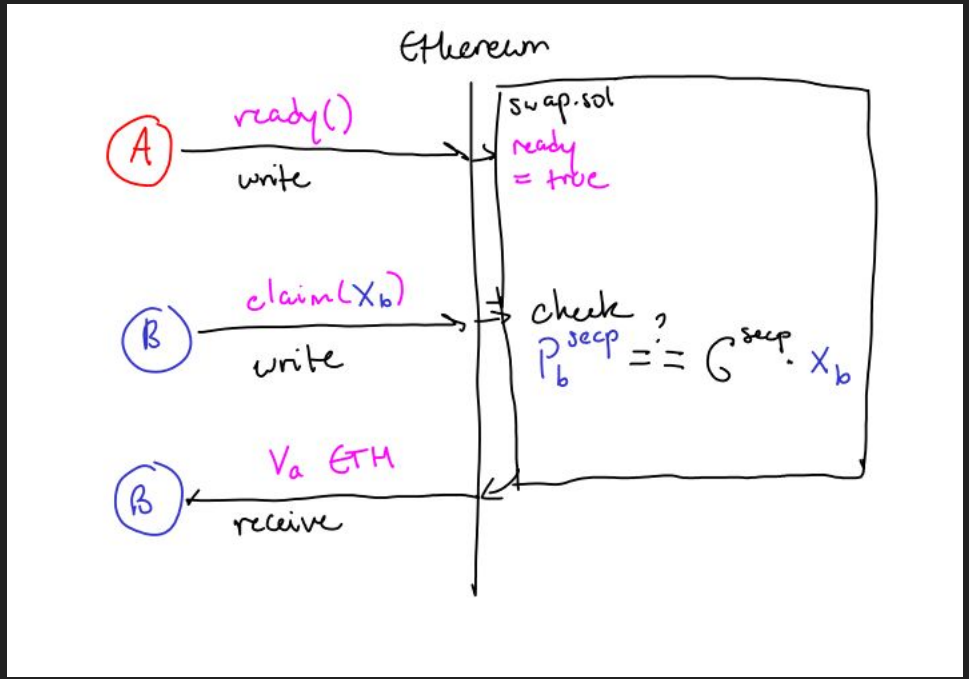
3. Bob verifies contract looks good, locks XMR in (ed25519) monero address `P_a + P_b`



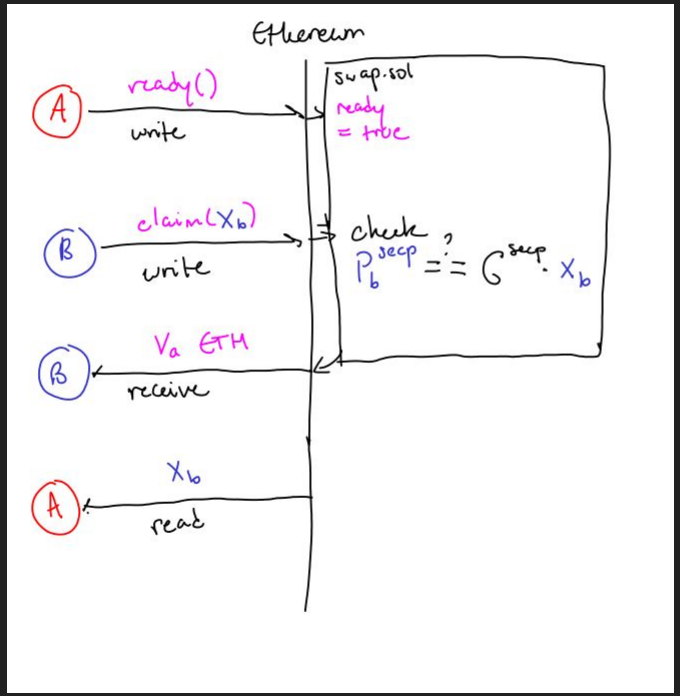


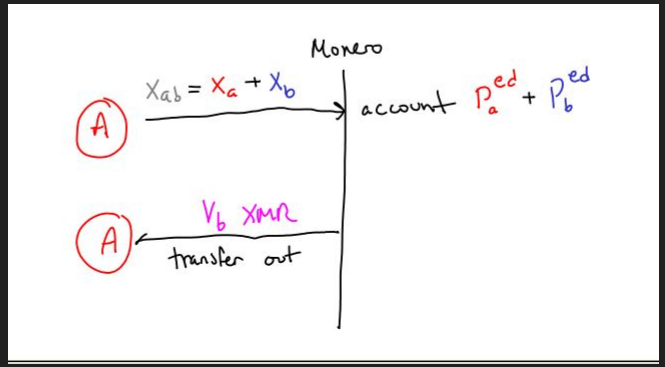
4. Alice sets contract to “ready”, allowing Bob to claim ETH from it

a. Bob claims by passing `x_b` to the contract
b. This is the “atomic” part - on reveal of `x_b`, Alice can claim XMR account `P_a + P_b` since the private key is `x_a + x_b`



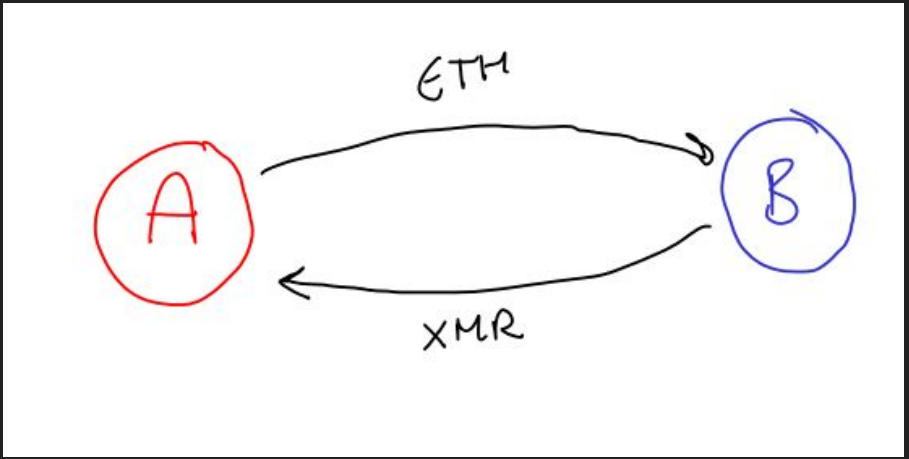
5. Alice now owns private key to locked Monero - swap complete!



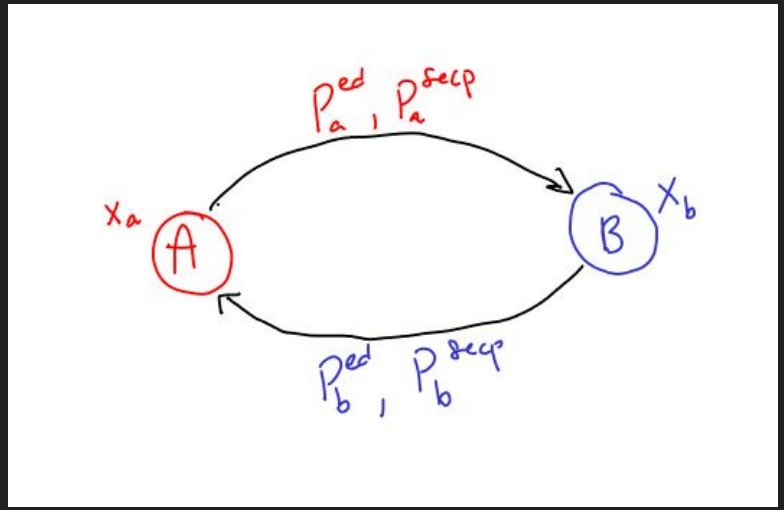


the protocol: unhappy (refund) path

- Alice: has ETH, wants XMR
- Bob: has XMR, wants ETH

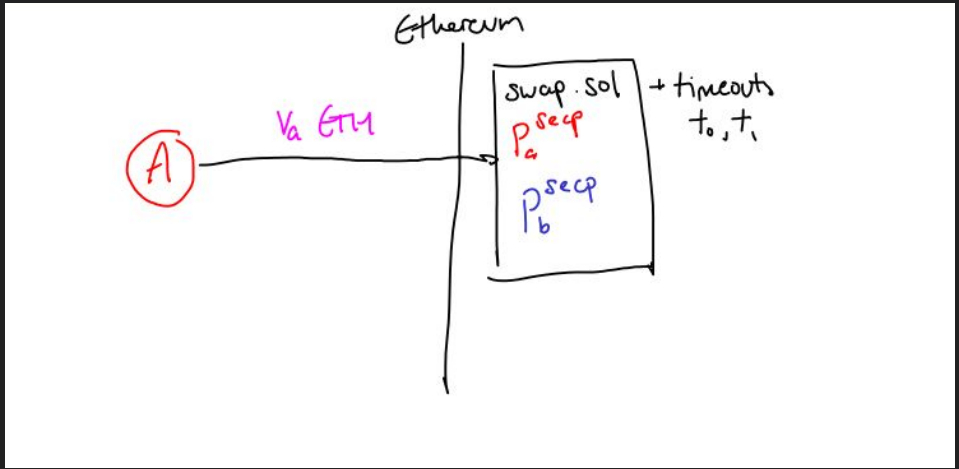


1. Alice and Bob meet and agree on the amount to swap
    a. They generate one-time swap secret keys `x_a` and `x_b`
    b. From their secret, they each generate a secp256k1 key (for Ethereum) and an ed25519 key (for Monero)
    c. They send these to each other over the network



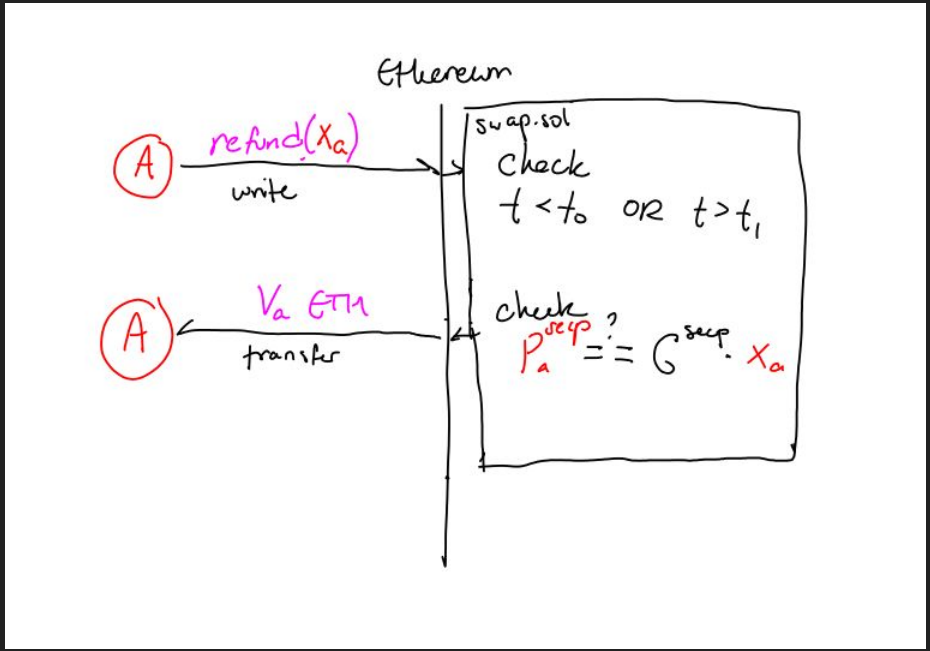
2. Alice locks ETH in a smart contract that stores secp256k1 `P_a` and `P_b`

a. Contract also has two timeouts `t0` and `t1`, where initiation time < `t0` < `t1`
b. A refund must be initiated by Alice by revealing `x_a`
c. Refund can be done *only* before `t0` and after `t1`



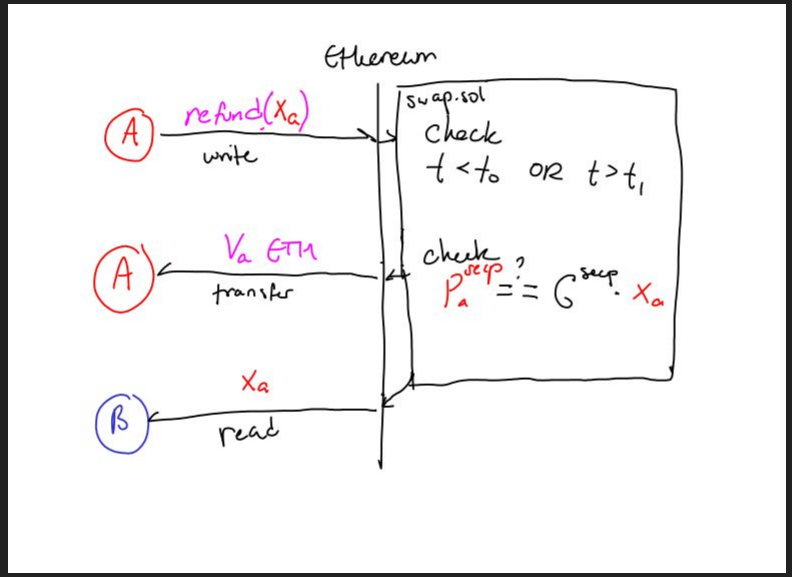
3. Case 1: Alice locks ETH, but Bob goes offline

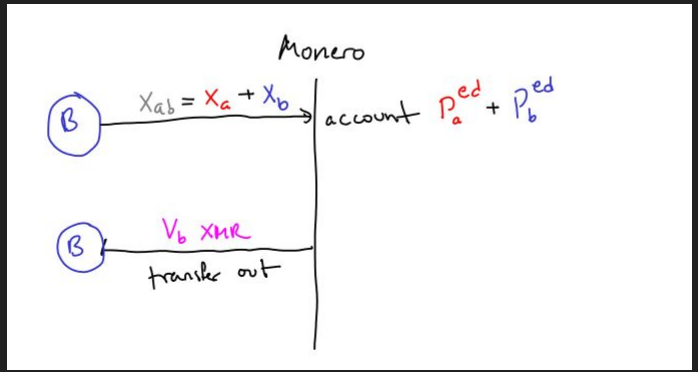
a. Alice refunds before `t0`, revealing `x_a`



3. Case 2: Alice locks ETH and Bob locks XMR, but Bob goes offline

a. Alice refunds after `t1`, revealing `x_a`
b. When Bob comes back online, he sees `x_a` on the ethereum chain - he now owns account with locked XMR `P_a + P_b` since the private key is `x_a + x_b`





privacy for atomic swaps

- Anonymity: hide who participated in the swap
- Confidentiality: hide amounts that were swapped
- Indistiguishability: hide that a swap happened at all; make swap transactions indistinguishable from “normal” transactions

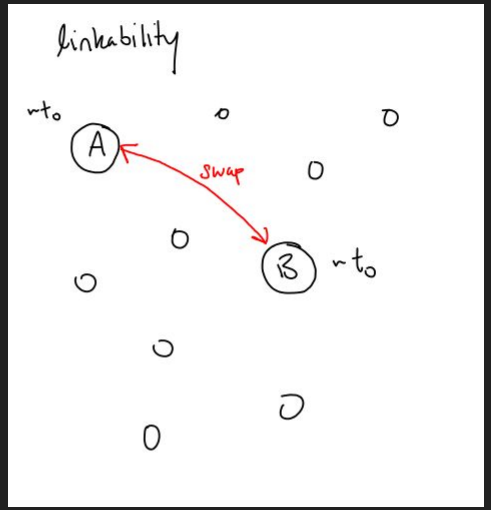
Privacy-Preserving Cross-Chain Atomic Swaps: https://par.nsf.gov/servlets/purl/10206409

privacy for atomic swaps

- Questions:
  - Network-level privacy vs chain-level privacy
  - What metadata can be leaked from watching the swap network?
    - Timing correlations
    - Who is interested in obtaining XMR or getting rid of XMR
    - Amounts offered
  - How does this affect the privacy of those doing swaps?
    - Linkability
    - Enumeration

linkability

- Can link 2 ETH accounts
- Can link two txs on different chains
- Can infer how much XMR swap recipient has

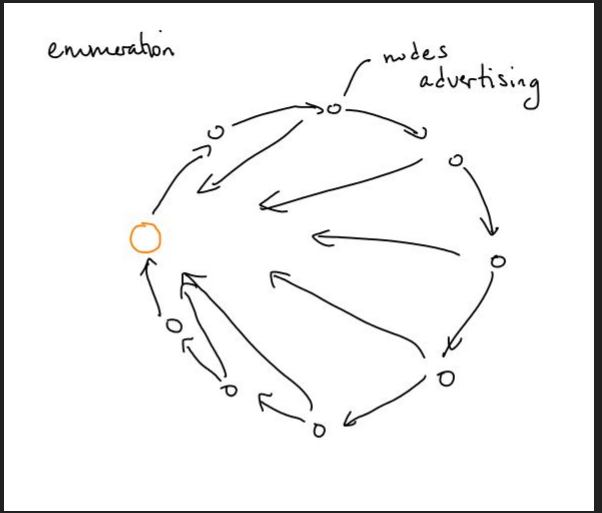


advertisement method

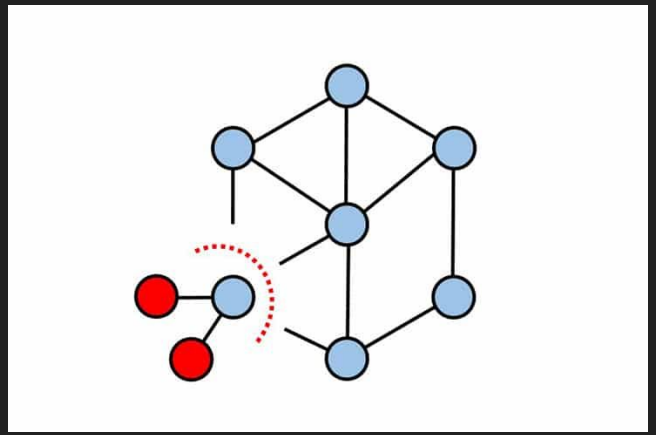
- How can swap providers advertise themselves?
  - Website (centralized)
  - DHT (decentralized)
  - Gossip network (decentralized)

enumeration

- Network-level metadata leakage
- Can search for all IPs offering or seeking a specific coin



potential attacks



- Depending on offer advertising method, can create many false offers
- Could grief XMR seeking nodes
- Much harder w/ decentralized advertisement methods that prevent eclipse attacks

https://assets-global.website-files.com/60540b6d30224a7cb015203a/60b8b424cb6dfebeab0e1227_what-is-an-eclipse-attack.jpg

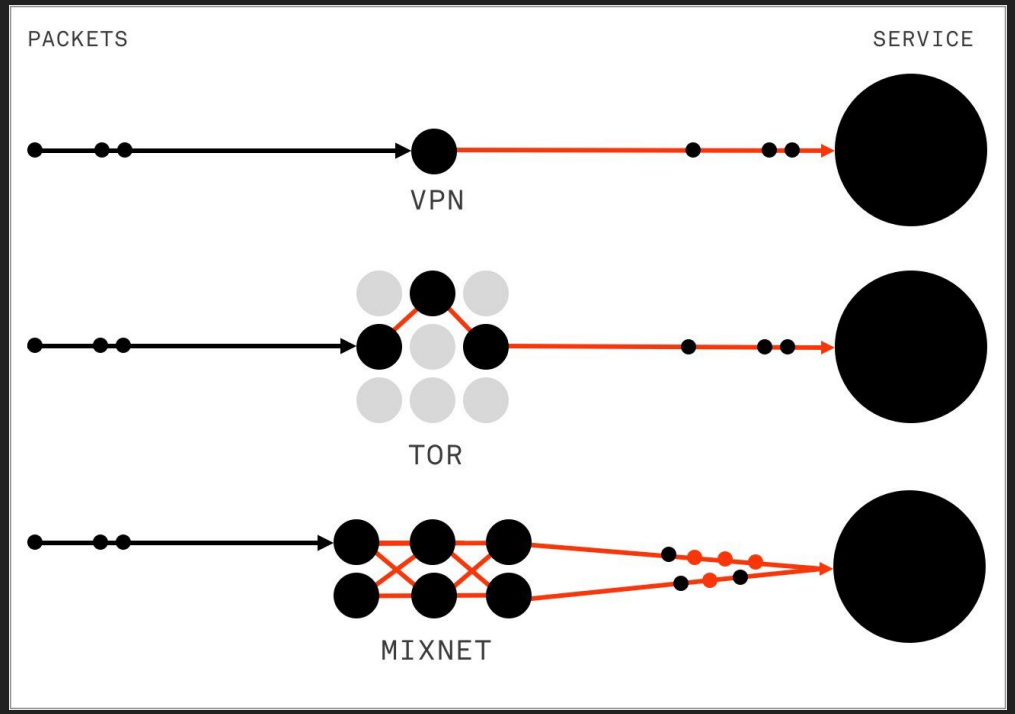
privacy for atomic swaps

- network-level goals
  - Sender-recipient anonymity: message sender shouldn’t know ID of receiver; message receiver shouldn’t know ID of sender
  - Anonymity of providers
  - Anonymity of those querying for providers
  - Confidentiality of swap amounts
- chain-level goals
  - Make swap txs indistinguishable from others
  - Confidentiality of swap amounts
  - Anonymity of swap participants

privacy for atomic swaps

- How can privacy be improved?
- On the network level:
  - VPN
  - Onion routing
  - Mixnets
  - Privacy-preserving DHT schemes
- On the chain level:
  - Timing delays for on-chain txs
  - L1 privacy
  - Scriptless swaps
  - Multi-party swaps

Network-level privacy improvements



https://pbs.twimg.com/media/ENm1-SDU4AA_G4N?format=jpg&name=large

future work

- Protocol v2
  - Gas improvements
  - Privacy improvements
  - Direct swaps for ERC20 tokens
- Network level privacy improvements
  - Discovery and advertisement
  - Sender-recipient anonymity

demo

end